Release Notes for the Cisco Secure Access Control System 5.0

Revised: July 10, 2009

OL-16251-01

These release notes pertain to the Cisco Secure Access Control System (ACS) release 5.0, hereafter referred to as ACS 5.0. These release notes provide information on the features, related documentation, and known caveats for functionality in this release.

This document contains:

Introduction

ACS is a policy-driven access control system and an integration point for network access control and identity management. ACS is the dominant enterprise network access control platform, and it is the administrative access control system for Cisco and non-Cisco devices and applications.

ACS 5.0 comprises an appliance, the Cisco 1120 Secure Access Control System (CSACS 1120), and the ACS Server software. This release of ACS provides new architecture and functionality on a standard Cisco Linux-based appliance.

Throughout this documentation, CSACS 1120 refers to the appliance hardware, and ACS Server refers to the ACS software.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

New and Changed Information

The ACS 5.0 release contains the following new and changed information:

New and Updated Features

ACS 5.0 provides the following new features:

- **Policy Model**—This revised, rules-based policy model allows you to address policy needs with greater flexibility.
- **Improved Management Interfaces**—The web interface has been completely redesigned and reorganized, and the command line interface (CLI) provides a text-based interface in which you can perform configuration tasks and monitoring.
- **Logging Functionality**—Logging functionalities such as integrated monitoring, reporting, and troubleshooting capabilities that are similar to those available in ACSView 4.0 are now supported.
- **Integration with External Identity Stores**—Improved integration with Windows Active Directory and Lightweight Directory Access Protocol (LDAP) back-end stores is supported.
- **Improved Runtime System**—ACS 5.0 supports a revised high-performance runtime system, based on field-proven code.
- **Distributed Deployment**—A new platform architecture, providing greatly enhanced centralized management in a distributed deployment, delivered as a Linux-based appliance.
- **Support for the Cisco Identity Solution Features—**This version of ACS supports the following Cisco Identity Solution features:
  - Wired 802.1x
  - Network Admission Control (NAC) RADIUS integration with Cisco NAC Appliance - Clean Access Manager.
  - Cisco TrustSec solutions
- **Shell Access Control**—ACS 5.0 supports shell access control to network devices via the TACACS+ protocol by using the Cisco IOS privilege level and TACACS+ per-command authorization.
- **Revised User Identity Store**—The use of revised ACS internal user and host identity store is supported.
- **Migration**—The initial version of migration tools for migrating data from ACS 4.x to ACS 5.0 is supported.

Features Not Supported

The following features are not supported in ACS 5.0:

- Integration with RSA server or RADIUS Token One Time Password (OTP) servers.
- Integration with SQL DB via ODBC, for external authentication and identity information.

- The following Extensible Authentication Protocol (EAP) methods are not supported:
  - LEAP
  - EAP-FAST/GTC
  - EAP-FAST/TLS
  - PEAP/GTC
  - PEAP/TLS
- Support for locally significant external resources (ID stores, and so on) in a distributed deployment.
- RADIUS and TACACS+ Proxy.
- Terminal server access control (port-based TACACS+ access control).
- Complete TACACS+ support for device administration (password change, and so on).
- RADIUS Virtual Private Network (VPN) and RADIUS-based device administration (for shell access to CLI for third-party network devices).
- ACS administrator and internal user password policies.
- Application access control for CiscoWorks applications.
- CSUtil features.
- Network access restriction to users whose Windows accounts have Windows dial-in permission.
- IP Pools Server feature.
- Support for defining the maximum number of simultaneous sessions for a user or user group.

Installation Notes

This section provides information on the installation tasks and configuration process for the ACS 5.0.

This section contains:

- Installing the CSACS 1120, page 3
- Running the Setup Program, page 5

Installing the CSACS 1120

This section describes how to install the CSACS 1120 Series appliance.

To install the CSACS 1120:

Step 1 Open the box containing the CSACS 1120 Series appliance and verify that it includes:

- The CSACS 1120 Series appliance
- Power cord
- Rack-mount kit
- Cisco Information Packet
- Warranty card
- *Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control System 5.0*

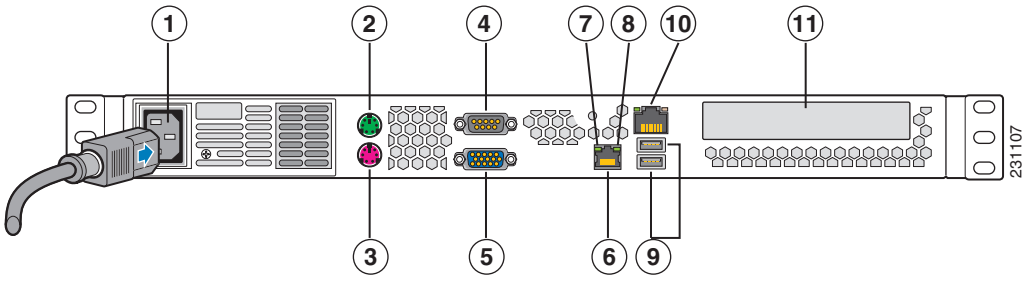
Step 2 Go through the specifications of the CSACS 1120 Series appliance. For more details, see Chapter 1 of the *Installation and Configuration Guide for the Cisco Secure Access Control System 5.0.*

Step 3 Read the general precautions and safety instructions you must perform before installing the CSACS 1120 Series appliance. For more details, see Chapter 2 of the *Installation and Configuration Guide for the Cisco Secure Access Control System 5.0* and pay special attention to all the safety warnings.

Step 4 Install the appliance in the 4-post rack, and complete the rest of the hardware installation. For more details on installing the CSACS 1120 Series appliance, see Chapter 3 of the *Installation and Configuration Guide for the Cisco Secure Access Control System 5.0.*

Step 5 Connect the CSACS 1120 Series Appliance to the network and appliance console. Figure 1 shows the back panel of the CSACS 1120 Series appliance and the various cable connectors.

Figure 1 CSACS 1120 Series Appliance Rear View



The following table describes the callouts in Figure 1.

1	AC power receptacle	**7**	NIC 2 port LED (activity)
2	PS/2 connector (video monitor)	**8**	NIC 2 port LED (link)
3	PS/2 connector (keyboard)	**9**	Two USB 2.0 ports
4	Serial (EIA/TIA-232) console port	**10**	NIC 1 port (10/100/1000 Mb/s) or Ethernet 0
5	Video Graphics Array (VGA) port	**11**	PCI adapter card slot (expansion)
6	NIC 2 (10/100/1000 Mb/s) port or Ethernet 1		

Note The ACS Server must use only the NIC 1 port on the appliance. Using NIC 2 may lead to software configuration problems.

Step 6 After completing the hardware installation, power on the appliance.

The first time you power on the appliance, you must run the setup program to configure the appliance. For more information, see Running the Setup Program, page 5.

Running the Setup Program

This section describes the setup process that installs the ACS Server.

The setup program launches an interactive CLI that prompts you for the required parameters. An administrator can use the console or a dumb terminal to configure the initial network settings and provide the initial administrator credentials for the ACS 5.0 server using the setup program. The setup process is a one-time configuration task.

To install the ACS Server:

Step 1 Power on the appliance.

The setup prompt appears:

```
Please type setup to configure the appliance
localhost login:
```

Step 2 At the login prompt, enter **`setup`** and press **Enter**.

The console displays a set of parameters. You must enter the parameters as described in Table 1.

Table 1 Network Configuration Prompts

Prompt	Default	Conditions	Description
Hostname	<*localhost*>	First letter must be an ASCII character. Length must be >2 but <20 characters. Valid characters are alphanumeric (A-Z, a-z, 0-9), hyphen (-), and the first character must be a letter.	Enter the hostname.
IPv4 IP Address	None, network specific	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255.	Enter the IP address.
IPv4 Netmask	None, network specific	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255.	Enter a valid netmask.
IPv4 Gateway	None, network specific	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255.	Enter a valid default gateway.
Domain Name	None, network specific	Cannot be an IP address. Valid characters are ASCII, any digit, hyphen (-), and period (.)	Enter the domain name.
IPv4 Primary Name Server Address	None, network specific	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255.	Enter a valid name server address.
Add/Edit another nameserver	None, network specific	Must be a valid IPv4 address between 0.0.0.0 and 255.255.255.255.	To configure multiple name servers, enter **`y`**.

Table 1 Network Configuration Prompts (continued)

Prompt	Default	Conditions	Description
Username	*admin*	The name of the first administrative user. You can accept the default or enter a new username. Must be >2 and < 9 characters, and must be alphanumeric.	Enter the username.
Admin Password	None	No default password. Enter your password. The password must be at least six characters in length and have at least one lower case letter, one upper case letter, and one digit. In addition: • Save the user and password information for the account that you set up for initial configuration. • Remember and protect these credentials because they allow complete administrative control of the ACS hardware, the CLI, and the application. • If you lose your administrative credentials, you can reset your password by using the ACS 5.0 installation CD.	Enter the password.

After you enter the parameters, the console displays:

```
localhost login: setup
Enter hostname[]: acs-server-1
Enter IP address[]: 209.165.200.225
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 209.165.200.1
Enter default DNS domain[]: mycompany.com
Enter Primary nameserver[]: 209.165.200.254
Add/Edit another nameserver? Y/N : n
Enter username [admin]: admin
Enter password:
Enter password again:
Pinging the gateway...
```

```
Pinging the primary nameserver...
Do not use `Ctrl-C' from this point on...
Appliance is configured
Installing applications...
Installing acs...
Generating configuration...
Rebooting...
```

After the ACS server is installed, the system reboots automatically. Now, you can log in to ACS with the CLI username and password that was configured during the setup process.

Note You can use this username and password to log in to ACS via the CLI only. To log in to the GUI, you must use the predefined username *ACSAdmin* and password *default*. When you access the GUI for the first time, you will be prompted to change the predefined password for the administrator. You can also define access privileges for other administrators who will access the GUI application.

Known Caveats

This section lists the known caveats for the ACS 5.0 release. Table 2 lists the contains known caveats in ACS 5.0. You can also use the Bug Toolkit on Cisco.com to find any open bugs that might not appear here.

Table 2 Known Caveats in ACS 5.0

Bug ID	Summary	Explanation
CSCsl61109	No IP validation in GUI and ACS Runtime (RT) process (leading '0').	**Symptom** When a remote target IP address such as 010.056.048.162 is created, the log delivery fails. **Conditions** This failure occurs when an invalid IP address such as 010 is used. The system does not accept such values. **Workaround** Use a valid IP format.
CSCso49849	Long string attribute values are not displayed.	**Symptom** For Authorization profiles, long string attribute values are not displayed in their entirety. **Conditions** Authorization profiles allow values to be defined for selected RADIUS attributes to be sent in an ACCEPT response. If it is a string attribute with a value of more than 50 characters, only the start of the string is displayed, but the full string contents are sent in the response. **Workaround** From the attribute list, select the definition that contains the long value and click **Edit**. The value for this entry is displayed in a text box. You can scroll within the text box to view the string.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsq56053	User unable to delete custom attributes in a large database.	**Symptom** If modifications are made to a user or host attribute while it is being deleted, errors occur. **Conditions** Requests sent to delete a user or host attribute can take several minutes to be performed if there are a large number of internal users or hosts defined. The attribute continues to be displayed in the list of configured attributes, even after the request has been sent. If another request is sent to modify the attribute, it causes instability of the attribute information. **Workaround** After sending a request to delete an attribute, wait for the process to complete before sending further requests to the user or host attributes.
CSCsq75381	Report parameters do not support wildcards.	**Symptom** Wildcards cannot be used while entering values for report parameters. The reports display exact matches for the specified report parameter values. **Conditions** This occurs for all reports. **Workaround** To use a wildcard: 1. Click **Select**. 2. Use the search filter in the dialog box to search for similar entries. 3. The search filter accepts the (*) wildcard.
CSCsq83529	External Policy fails if Cisco Clean Access Manager (CCA) is configured with a hostname containing unprintable characters.	**Symptom** A communication error occurs when ACS accesses the External Policy Server using the GAMEv2 protocol. **Conditions** This error occurs when the CCA is configured: • As an External Policy Server. • With a hostname that contains unprintable characters such as a backspace. **Workaround** Reinstall the CCA and ensure that you do not press backspace while typing the hostname.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsq84312	On Funk/EAP-FAST after change password fails user cannot log in.	**Symptom** If the supplicant enters a non compliant password, the following error is displayed: `change password failed` but the request for a new password is not displayed. **Conditions** This error occurs on Funk 4.02.0.2000 on XP. When the supplicant enters a non compliant password the following error is displayed: `change password failed` but the request for a new password is not displayed. Instead, the supplicant uses the previously entered non compliant new password for authentication and does not use the previously entered valid password. If the supplicant uses the previously entered non compliant new password for authentication, the same error occurs. **Workaround** Restart the Odyssey service on the supplicant system. **Note** This bug applies to only a supplicant.
CSCsq93350	The DenyAccess and PermitAccess options can be enabled simultaneously.	**Symptom** In addition to the DenyAccess profile, if you select Authorization profiles as results, they are ignored. **Conditions** From the results of the Network Access Profiles (NAP), you can select multiple Authorization profiles to determine the RADIUS attributes that are to be present in an ACCEPT response. If you simultaneously select the reserved profile DenyAccess, the contents of the other profiles are ignored. **Workaround** None. **Note** To deny access in an authorization, it is recommended that you select only the DenyAccess profile.
CSCsr01154	The Out of Memory exception stores the full migration report only on a file.	**Symptom** When migrating a large database of over 100,000 users and 50,000 devices the `OutOfMemory` exception is generated. **Conditions** This exception occurs when you migrate a large database containing more than 100,000 internal users and 50,000 devices. **Workaround** Migrate each object type separately. For example, migrate the users and then the devices.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsr11124	When choosing a user for RADIUS, the MAC address is listed.	**Symptom** When generating a RADIUS authentication report, if you choose User as the report parameter and click Select, the search lists usernames and MAC addresses. **Conditions** This issue occurs when you choose User as the report parameter and click Select. This applies to RADIUS authentication reports. **Workaround** None.
CSCsr13884	When the Common Name (CN) contains certain characters, the Signing ACS Certificate request fails.	**Symptom** The Certificate Authority (CA) fails to sign the ACS certificate. **Conditions** This issue occurs: • When the CN uses characters other than the following: a..zA..Z0..9\+/-)(.,:=? • If the CA is invoked using the **openssl ca** command. **Workaround** To avoid this problem, do one of the following: • Use only these characters in the CN: A-Z, a-z, 0-9, and \ + / -) (. , : = ? • Use the **openssl x509** CA command.
CSCsr24674	Exporting a report to PDF generates formatting issues.	**Symptom** While viewing a report if you click the Print button, you can choose the option of exporting the report to PDF. But the PDF export generates several formatting issues such as: • The page length and width will not match the report as viewed in the browser. • The report parameters will not appear. **Conditions** None. **Workaround** Select HTML as the export option and not PDF.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsr60433	Unable to delete a Certification Revocation List (CRL).	**Symptom** No direct way to deactivate a CRL list. **Conditions** Define a CRL list. **Workaround** To avoid this issue: 1. Untrust the CA certificate. 2. Click the **Submit** button. 3. Trust the CA certificate again. This clears the CRL information for the CA.
CSCsr62965	From the remote desktop the migration tool is unable to connect to the ACS internal database.	**Symptom** During the extract and export phases, the migration tool cannot connect to the ACS 4.x database. **Conditions** This issue occurs when you use the remote desktop to connect to the migration machine to run the migration utility. **Workaround** Run the migration utility on the migration machine; or, use VNC to connect to the migration machine.
CSCsr68048	Changes to CSACS 1120 hostname trigger ACS restart without warning	**Symptom** When you use the CLI to modify the hostname, ACS restarts without giving you an option to roll back. **Conditions** This error occurs when you use the CLI to update the hostname. **Workaround** During the setup process, set the interface and do not modify it later.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation

CSCsr68136	CSACS 1120 IP address change triggers ACS restart without warning	**Symptom** When the CLI is in configuration mode and if you use it to modify an interface IP address, ACS restarts without any warning.
		
		Conditions When you use the CLI to update an IP address, ACS restarts displaying the following:
		`ACS-1-v5/admin(config)# interface gigabitEthernet 0`
		`ACS-1-v5/admin(config-GigabitEthernet)# ip address 10.86.155.89 255.255.255.0`
		`IP Address was modified.`
		`ACS is restarting and a new HTTP certificate will be generated.`
		`Stopping ACS ..`
		`Starting ACS ....`
		`To check the status of the ACS processes, use the 'show application status acs' command.`
		`ACS-1-v51/admin(config-GigabitEthernet)# exit`
		`ACS-1-v5/admin(config)# exit`
		`ACS-1-v51/admin#`
		
		Workaround During the setup process, set the interface and do not modify it later.

CSCsr74090	ADE OS password recovery generates an error handle 64-bit address.	**Symptom** When you perform a password recovery using the DVD and type options 3 or 4, the following error appears: `PCI: Unable to handle 64-bit address space for` is displayed. But the password recovery operation succeeds. **Conditions** This error occurs when you use the DVD for password recovery. **Workaround** None.
CSCsr94065	No log messages can be viewed for monitored rules.	**Symptom** Unable to view the monitored rules log messages. **Conditions** Rules match when the monitored-only setting is enabled. **Workaround** To view the monitored rules log messages, in the Policy Diagnostics scope, set the log severity to INFO.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsu33401	When exporting reports, the default file name to save the file is *iv*.	**Symptom** Select **Reports > Catalog > AAA Protocol > RADIUS Authentication.** 1. Enter the required query and run the report. 2. In the displayed report, click the **Export Report Icon**. The Word option is selected by default. 3. Click **OK**. The default filename iv.doc is used. **Conditions** This occurs for all reports. **Workaround** From the file download popup: 1. Choose **Save**. 2. Overwrite the iv.doc filename with a user-defined filename. 3. Click **Save** to save the file.
CSCsu69983	Restoring a configuration disconnects deployment and causes replication to fail.	**Symptom** After restoring a backup database to a primary database, the deployment is disconnected. **Conditions** When a backup database is restored, the database no longer contains correct deployment information for the secondary instance that belonged to the previous database. To avoid sending replication updates to the wrong secondary instances, the underlying replication communication system is changed so that only reconnected or newly registered Secondaries will receive replication updates. **Workaround** After a database restore, you must perform a hardware replacement for each secondary instance to reconnect to the primary instance.
CSCsu84710	ACS Authentication Activity generates Error #2032 after a few hours.	**Symptom** While viewing the dashboard, if the page remains open for more than for 45 minutes, the following error is displayed in the ACS Authentication Status graph: `faultCode:Server.Error.Request faultString:'HTTP request error'` **Conditions** This error occurs when the ACS dashboard page remains open for more than 45 minutes. **Workaround** In the left navigation pane, click the Dashboard link to refresh the dashboard.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsv12516	When FullSync is performed over WAN from secondary server, it hangs for 90 minutes.	**Symptom** If the admin is triggered on the secondary server when it is in FullSync, the secondary server hangs and the GUI becomes non-responsive. **Conditions** This issue occurs when: 1. The deployment is performed over WAN. 2. The primary is under stress. **Workaround** To avoid this issue: 1. Restart the secondary server. 2. Initiate a FullSync when no there is no stress on the primary.
CSCsv17209	Nested Groups with machine authentication do not work.	**Symptom** Unable to retrieve nested groups from Active Directory for machines. **Conditions** If a machine in Active Directory is assigned to a group (for example, group NY) that is a member of another group (for example, group US), the related group (US) cannot be retrieved during machine authentication or lookup. **Workaround** To retrieve the nested group, the machine must be added as a member of this group.
CSCsv23653	Authorization profile VSA attribute longer than 247 sends invalid packet.	**Symptom** RADIUS packet is sent with invalid Cisco-AV-Pair attribute. **Conditions** This problem occurs when a RADIUS Network Access Authorization profile VSA attribute such as Cisco-AVPair is configured with a value greater than 247 characters. **Workaround** Limit the length of the VSA value to fewer than 247 characters.
CSCsv23710	Shell profile attribute longer than 255 characters sends invalid packet.	**Symptom** A dysfunctional TACACS+ packet is sent if the actual attribute length is truncated to modulus 256. The packet can become blank if the residue is equal to zero. **Conditions** When a Shell-profile attribute such as Cisco-AV pair, is configured with a value greater than 255 characters. **Workaround** Limit the length of the configured Shell profile attributes to fewer than 256 characters (when combined with the length of the name of the attribute + 1).

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation

CSCsv27278	When Active Directory is disabled, ACS authenticates even if advanced option is REJECT.	**Symptom** If a query is performed when the Domain Controller (DC) is disabled, the following error is not displayed:
		`server unreachable`
		Instead, the following error is displayed:
		`user not found`
		For example, if Active Directory is used to retrieve attributes only when the the DC is down, the `process failure` fail-open is not displayed.
		Conditions This issue occurs when the DC is down and Active Directory is used for querying attribute retrieval.
		Workaround None.

CSCsv27384	Adding a new Active Directory without removing the previous Active Directory configuration.	**Symptom** The Active Directory definition can contain attributes and groups that are not applicable to the defined domain. **Conditions** When ACS is connected to a specific Active Directory domain, you can select groups and attributes that are specific to that domain. If the administrator enters a new domain, the defined groups, attributes, and definitions from the previous domain are not deleted, but are retained. **Workaround** Before changing to a new domain, clear all existing configurations using the Clear Configuration option on the Active Directory page.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation

CSCsv29628	CSACS 1120 CLI shows logging inconsistencies.	**Symptom** When a **show** command generates lengthy output, the option `--More--` appears at the bottom of the screen. For example, if the h key is used, it generates a lengthy UNIX help output which displays the **more** command as shown below:
		`Most commands optionally preceded by integer argument k.`
		`Defaults in brackets. Star (*) indicates argument becomes`
		`new default.`
		`---------------------------`
		`<space> Display next k lines of text [current screen size]`
		`z Display next k lines of text [current screen size]*`
		`<return> Display next k lines of text [1]*`
		`d or ctrl-D Scroll k lines [current scroll size, initially 11]*`
		`q or Q or <interrupt> Exit from more`
		`s Skip forward k lines of text [1]`
		`f Skip forward k screenfuls of text [1]`
		`b or ctrl-B Skip backwards k screenfuls of text [1]`
		`' Go to place where previous search started`
		`= Display current line number`
		`/<regular expression> Search for kth occurrence of`
		`regular expression [1]`
		`n Search for kth occurrence of last r.e [1]`
		`!<cmd> or :!<cmd> Execute <cmd> in a subshell`
		`v Start up /usr/bin/vi at current line`
		`ctrl-L Redraw screen`
		`:n Go to kth next file [1]`
		`:p Go to kth previous file [1]`
		`:f Display current file name and line number`
		`Repeat previous command`
		Conditions When the user is logged into the CLI and types the **show** command such as one of the following:
		• **show logging**
		• **show tech-support**
		Workaround None.

CSCsv36400	Error occurs if special characters colon (:), equal sign (=), vertical bar (|) used to create NDG and UserGroup.	**Symptom** An import error occurs for an object containing special characters such as colon (:), equal sign(=), or vertical bar (|). **Conditions** An object name that includes special characters such as colon (:), equal sign(=), or vertical bar (|). **Workaround** Add these objects manually to ACS 5.0.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsv39533	Attributes related to authentication methods confuse usability issues.	**Symptom** ACS 5.0 has four attributes that may confuse clients: • EAP Tunnel • EAP Authentication • Authentication Method • UseCase This occurs when some of the values overlap, which creates difficulty in detecting which attribute or value belongs to a specific use case. **Conditions** A rule that is constructed with the condition AuthenticationMethod=Lookup, does not identify a specific use case. For example, it matches MAB, User/Machine Auth with PAC, T+ ATZ and SessionResume/Fast Reconnect. **Workaround** To enable you to identify MAB requests, you need to add conditions based on the UseCase attribute that is located in the system dictionary. The UseCase attribute should be the first rule so that it will not impact other use cases.
CSCsv45016	Error is generated when special characters are used in report parameters.	**Symptom** When specifying report parameters before running a report, if you enter special characters in one or more of the parameters, the report is not generated and an error message appears. **Conditions** When specifying special characters such as *`~!@#$%^&*()^{}[];:"'* in one or more of the report parameters. **Workaround** None.
CSCsv49164	Importing of users when there are a large number of errors.	**Symptom** It takes several minutes for the results of the import process to display. **Conditions** The import of users , hosts, or devices can take up to 500 records as input. If errors occur for many or all of the records, it takes several minutes for these errors to be displayed. **Workaround** If a number of errors occur during the import process, wait for a few minutes until the process completes and all the errors are displayed.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsv49899	When ACS instance is set to local mode, system alarm on dashboard is generated.	**Symptom** When an instance of ACS is set to local mode, the log collector stops collecting syslog messages from this instance and displays a system alarm: `System Alarm [Collector] Message received from an unregistered ACS Server.` **Conditions** This issue occurs when an instance of ACS is set to local mode. **Workaround** None.
CSCsv65146	Dashboard Alarm section must be properly aligned to fit frame.	**Symptom** When viewing the dashboard, the alarms section overflows towards the right of the browser. This overflow occurs as the alarms section is wider than the overall size of the dashboard. **Conditions** None. **Workaround** To avoid this issue, do one of the following: • Increase the size of the browser. • Increase the resolution of the monitor to 1280 x 1024 pixels or higher.
CSCsv65225	The health summary of the ACS instance for secondary server is not updated.	**Symptom** While viewing the health summary of the ACS instance, the process status shows the process as running even if the process is not active. **Conditions** This issue occurs while viewing the health summary of the ACS instance. **Workaround** None.
CSCsv65444	Monitoring and Reporting log section contains incorrect steps on the Advance option.	**Symptom** The Monitoring and Reporting log section mentions that ACS continues with Advance options even after the Reject or Drop options are selected; these steps are incorrect. **Conditions** Configure the ACS **Access-services > Identity > Advance** option to Drop or Reject the three drop-down options. **Workaround** None.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsv73390	Password change fails if invalid credentials are used initially.	**Symptom** When a Change-Password subsequence is performed while authenticating via EAP-FAST using the CSSC 4.2 supplicant, it fails if you use an invalid password the first time. If you retry using a valid password, the process fails. **Conditions** When an invalid password is used for the first time irrespective of the Identity Store (Internal or Active Directory) used to authenticate the user. **Workaround** To avoid this issue, do the following: • Try a new EAP-FAST authentication. • When performing the Change-Password subsequence, ensure that you enter a valid password the first time.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsv78191	Incorrect Failure Reason displayed when password changed during anonymous provisioning	**Symptom** When a Change-Password subsequence is performed during the execution of a successful EAP-FAST PAC-provisioning sequence, an incorrect Failure Reason is displayed. **Conditions** When an EAP-FAST PAC-provisioning request is processed and the following steps have been performed during the process: • The relevant Identity Store detects that the user's password has expired. • An MSCHAPv2-level Change Password operation is performed during this process. • Valid credentials are supplied. • The password is successfully changed. • The PAC is successfully provisioned. an incorrect Failure Reason is displayed. The specific Failure Reason displayed, depends on the Identity Store that is used to authenticate the user. For example, if the Identity Store used to authenticate the user is Active Directory, the Failure Reason displayed is: `User authentication against Active Directory failed as user password has expired.` This Failure Reason is incorrect as: – No failure occurs. – It is normal for a user password to expire. **Workaround** There is no workaround for this. To check if the PAC-provisioning operation was successful, you must verify that the report contains the following steps: • Approved EAP-FAST client PAC request. • Successfully finished EAP-FAST PAC provisioning or update. • Prepared RADIUS Access-Reject after successful in-band PAC provisioning. Once this is verified, you can safely ignore the incorrect Failure Reason that is displayed.
CSCsv86093	Assign default values for devices when creating new a NDG hierarchy.	**Symptom** An error occurs when saving an edited network device. **Conditions** If existing network devices are edited after adding a new Network Device Group (NDG), an error occurs when the NDG is saved. **Workaround** To avoid this error, when editing the newly added network device, ensure that you enter a value in the empty field before saving the NDG.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsv88662	Reports are not displayed in ACS View.	**Symptom** When the ACS monitoring and reports application is launched, the reports are not displayed in the reports catalog or in the default favorite reports. **Conditions** This issue occurs if the administrators name contains special characters such as !@#$%^&*()\/"'[]{} **Workaround** Do not use special characters in administrator names.
CSCsv93091	After the ACS hostname is changed ACS does not rejoin Active Directory.	**Symptom** After the ACS hostname is changed, Active Directory authentications fail. **Conditions** When the ACS hostname is changed via the CLI, Active Directory authentications fail. **Workaround** If you have to change the ACS hostname, first change the hostname in Active Directory and then change the ACS hostname via the CLI.
CSCsv94620	During migration, Analyze and Export phases take a long time for a large number of MABs.	**Symptom** During migration, it takes a long time to extract, analyze, and export MAB data from the NAP table in ACS 4.x **Note** These processes may take up to 1 hour to complete. **Conditions** This issue occurs when there many MAC addresses defined in the NAP table. **Workaround** None. You must wait for the process to complete.
CSCsv94627	TACACS+ failed authentication errors not recorded in Failed Attempts log.	**Symptom** Failed Attempts logs do not record TACACS+ authentications that display the TACACS authentication status `ERROR (status code 0x07)`, instead of `"FAIL" (status code 0x02).` **Conditions** This issue occurs when TACACS+ authentications display the TACACS authentication status `ERROR (status code 0x07).` **Workaround** Check the TACACS+ Diagnostics logs where the failed log is recorded.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsv94911	Previous import pop-up causes IE 7 import to stop at initializing state.	**Symptom** The popup window for the import progress continues to remain in the initializing state even though the import process is running (this depends on the csv validity). **Conditions** Open a new import session while the previous import progress popup is still open. **Workaround** To avoid this issue, do the following: 1. Close all import pop-ups and restart the process. 2. Verify that the items you tried to import previously were not imported. You must ensure this for the following reasons: • The previous import process may have worked even though the progress pop-up was not functioning. • To avoid re-importing the items. **Note** Before importing any items, you must disable the pop-up blocker for ACS 5.0. If you do not disable the pop-up blocker, the import process will generate abnormal behavior.
CSCsv96439	Incorrect encoding of US Robotics RADIUS VSA attributes.	**Symptom** US Robotics RADIUS Vendor Specific Attributes (VSAs) that are configured and sent to NAD, are sent invalid. When this occurs, NAD does one of the following: • Fails to recognize them as valid VSAs. • Recognizes them as other valid VSAs. **Conditions** If you configure ACS to send US Robotics RADIUS VSAs (vendor ID = 429) to NAD, invalid RADIUS VSAs are regularly sent and the value of the Vendor Type field (see RFC 2865, section 5.26) is incorrectly truncated to its least significant byte. This issue is applicable to most US Robotics RADIUS VSAs that contain a Vendor Type greater than 255. When NAD receives these VSAs, they display an incorrect Vendor Type value that is less than or equal to 255. **Workaround** To avoid this issue, do not configure ACS to send US Robotics RADIUS VSAs to the NAD.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsv97503	Monitoring and Reporting does not change severity log view based on ACS configuration.	**Symptom** When configuring AAA diagnostic logs for a severity level that is different from the default level (WARN), Monitoring and Reporting does not show these logs. **Conditions** This issue occurs when: • Configuring ACS from System Administration. • Viewing the logs in Monitoring and Reporting by navigating to **Reports > Catalog > AAA Protocol**. **Workaround** To avoid this issue, do one of the following options: Option 1 1. Choose the report you require by clicking the radio button next to it. 2. Click the **Run** button. 3. Choose the option **Query and Run**. 4. In the Run Report window, choose the Severity level. 5. Click the **Run** button. Option 2 1. Choose the report you require by clicking the radio button next to it. 2. Click the **Add To Favorite** button. 3. Choose a name for the report. 4. From the drop-down list, choose the Severity level. 5. Click the **Add To Favorite** button. 6. You can view the report by navigating to **Reports > Favorites**.
CSCsw16668	MAR is not applied to user machine that was rejected during authorization.	**Symptom** If a user machine is rejected during authorization, MAR is not applied to it. **Conditions** This issue occurs when machine authentication is successful but fails in ATZ. You must configure the machine to check MAR and verify whether the user ATZ based on MAR is successful or has failed. **Workaround** None.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw18375	TACACS+:User condition does not work when T+ ASCII authentication used.	**Symptom** When T+ ASCII authentication is used, the TACACS+:User condition does not work. **Conditions** If you choose the attribute TACACS+:User, the Identity Policy does not work because the username is saved in Acs::UserName and not in TACACS::User. **Workaround** Choose the UserName attribute from the System dictionary and not from the TACACS dictionary.
CSCsw18800	DBs attempting to delete an identity sequence being used are removed.	**Symptom** When a specific identity sequence is selected, authentications fail and replications stop. **Conditions** When you attempt to delete an identity sequence that is referenced from a policy, the request to delete fails and an error is generated indicating that the sequence is referenced. After the error is generated, the identity sequence no longer references any databases. This causes authentications to fail and replications to stop. You must avoid deleting identity sequences and make modifications to existing sequences. After the error is generated, you must restore database definitions to the sequence and then perform full synchronization for all the secondaries in the deployment.
CSCsw18978	If T+ authentication fails, a T+failure status is not displayed.	**Symptom** When the Identity Policy authentication fails with a DenyAccess, the TACACS+ authentication status is displayed as TACACS+ Error authentication instead of TACACS+ Failure authentication. **Conditions** This issue occurs when the Identity Policy authentication and the TACACS+ authentication fails with a DenyAccess. **Workaround** None.
CSCsw19773	T+:Remote-Address condition does not work with T+ ASCII auth	**Symptom** The T+:Remote-Address condition does not work with T+ ASCII auth (except in the service selection policy). **Conditions** To avoid this issue, define the TACACS+:Remote-Address attribute in a policy and perform the T+ ASCII authentication. **Workaround** None.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw21730	Authorization profile cannot save dynamic dACL attributes in multiple stores.	**Symptom** When Authorization profile references for a dynamic attribute from an ID store are saved, it fails and does not display an error. **Conditions** Authorization profiles can reference an attribute from an ID store where the dACL name is retrieved. If the name of the referenced attribute appears in other identity stores, the references are not saved and an error is not displayed. **Workaround** To avoid this issue, you must store the dACL name in an attribute with a unique name, across stores.

CSCsw21781	Authorization policy displays the following error:
	`required container of HierarchyLabel is empty error`
		Symptom The secondary server GUI displays the following error:
		`Required container of HierarchyLabel is empty.`
		
		Conditions Define two policies on the primary server. For one of the policies, add an *iin* to one of its operand conditions and register a secondary server to the primary server. After registering the secondary server, go to the primary server and update the policy that does not include the NDG. Check the other policy on the secondary server; the following error message is displayed:
		`required container of HierarchyLabel is empty error`
		
		Workaround To avoid this issue, perform a FullSync for the server that displayed the error.

CSCsw21908	ACS Instance Health Summary check does not display AdClient status.	**Symptom** Monitoring and Reporting does not report the AdClient status. **Conditions** When a Monitoring and Reporting ACS Instance Health Summary check is performed, the report does not display the AdClient status. If the **show application status acs** command is used via the CLI, it displays the AdClient status as running. **Workaround** To avoid this issue, you must use the **show application status acs** command via the CLI.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw22035	Monitoring and Reporting displays inconsistencies in ACS Instance Health Summary	**Symptom** In Monitoring and Reporting, when you view the status report for a particular ACS using the ACS Instance Health Summary report, several inconsistencies are displayed for the given time range such as the last 30 days. **Conditions** When the time range selection is **Time Range: November 2, 2008 - December 1, 2008**, the following inconsistencies are displayed: • The Time vs Utilization & Latency chart displays results only for the period of Nov 26 to Dec 1, instead, of the previous 30-day period, with breaks in the missing dates. • The Time vs Utilization & Throughput chart displays results only for the period of Nov 26 to Dec 1, instead of the previous 30-day period, with breaks in the missing dates. • The downtime process window displays results for only the previous day even when it is repeated every five minutes and does not display results for the 30-day period. • If ACS is not running the collector, the down time process displays the following message: `Process Down Time: No results were found` However, the view components that are not running are not displayed. **Workaround** None.
CSCsw22197	The Identity and Authorization Policy page should not contain T+ Accounting Attributes.	**Symptom** The Identity Policy and Authorization Policy options should not contain T+ Accounting Attributes. **Conditions** This issue occurs when the administrator chooses the T+ Accounting Attributes option from the Identity Policy page or the Authorization Policy page. **Workaround** None.

CSCsw22403	AAA authentication should not be enabled via the ACS CLI.	**Symptom** When you log in to the ACS CLI via SSH , the aaa prompt is displayed while in configuration mode. This prompt should not appear on ACS servers.
		
		Conditions The prompt displays:
		`acs5-cars15/admin# configure`
		`Enter configuration commands, one per line.  End with CNTL/Z.`
		`acs5-cars15/admin(config)# ?`
		`Configure commands:`
		`aaa Authentication options`
		
		Workaround To avoid this issue, you must not use the aaa prompt while in configuration mode.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw27331	Local mode Save Configuration Change Report does not work in IE6 or IE7.	**Symptom** When you click the Save Configuration Change Report button, the standard pop-up dialog box for the browser download opens and displays the following options: • Open • Save • Cancel When you choose Open, the configuration change report (csv) directly opens in excel. In excel, you can save the report to a csv file on the clients machine. If you use IE6 or IE7 to open the csv file, the following pop-up error message is displayed: `Internet Explorer cannot download <document.pdf> from <server>` **Conditions** When certain versions of IE6 or IE7 are used to open Microsoft Office documents such as .csv files, an error message is displayed. For more details about this error, see the Microsoft Support website. **Workaround** To avoid this error, do one of the following: • Save the .csv file to the disk first, before trying to directly open it. • Use the supported hotfix that is available. • Ensure that the Do Not Save Encrypted Files check box is unchecked. • Ensure that the server does not send the Cache-Control: No Store or the Cache-Control: No Cache header. • Use a HREF to load the document.
CSCsw27484	EAP authentication displays an error when a username is not used.	**Symptom** The following error message does not contain sufficient detail: `1500 Invalid EAP payload dropped` **Conditions** This error occurs when you do not use a username to authenticate with EAP tunnel. **Workaround** None.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw31817	The **show cdp neighbors** command displays the CSACS 1120 platform as CADE1010.	**Symptom** The ACS machine platform and version that is displayed by the CDP protocol is incorrect. **Conditions** When you perform a CDP query using the devices directly connected to the ACS server, the ACS version and platform that is displayed is incorrect. **Workaround** To avoid this issue, log in to the CLI and run the following commands: • **show version**—To display the CSACS OS version. • **show udi**—To display the hardware version.
CSCsw33239	Some VPN3000 attributes are not sent to the Syslog.	**Symptom** The RADIUS response contains the VPN3000 attribute CVPN3000/ASA/PIX7.x-Client-Type-Version-Limiting attribute but the syslog does not contain this attribute. **Conditions** The CVPN3000/ASA/PIX7.x-Client-Type-Version-Limiting attribute must be sent in the RADIUS response. **Workaround** None.
CSCsw34484	Wrong online and replication status after changing IP.	**Symptom** After a secondary server reports online to the primary, the replication no longer displays the status as Updated in the Primary Instance Listing window. **Conditions** This issue occurs if the online status notification is not sent correctly. **Workaround** To avoid this issue, do one of the following: • Change a simple configuration setting to send the replication and correct the state. • Perform a FullSync to correct the state.
CSCsw36994	dACL greater than 32k prevents the extraction of other dACLs during migration.	**Symptom** If a dACL is greater than 32K, only part of it is extracted during migration. **Conditions** This issue occurs in ACS 4.x when a dACL is greater than 32K. **Workaround** None.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw45207	ACS uses only one CPU even if two CPUs are present.	**Symptom** An ACS server that is installed on VMWare does not utilize two CPUs and reduces performance. **Conditions** This issue occurs only for an ACS installed on VMWare. **Note** ACS supports VMWare free server and VMWare ESX. **Workaround** To avoid this issue, you must install ACS 5.0 patch 3:5.0.0.21.3
CSCsw48760	Error not displayed when adding ACS with hostname greater than 15 characters.	**Symptom** When the hostname is greater than 15 characters, the ACS connection to Active Directory fails. **Conditions** This issue occurs when you configure the ACS hostname with a value that is greater than 15 characters. **Workaround** To avoid this issue, you must configure the hostname with a value that is fewer than 15 characters.
CSCsw49110	CSACS 1120 reporting functions are not displayed or are dimmed.	**Symptom** A large number of Catalog options in the Run drop-down list are not displayed or are dimmed. **Conditions** When you navigate to **Monitoring & Reports > Reports > Catalog** and view the Catalog options, a large number of options in the Run drop-down list are not displayed or are dimmed. **Workaround** None.
CSCsw49137	If the primary DNS is not functioning, the Active Directory page is slow.	**Symptom** When the primary DNS server is not functioning and the secondary DNS server is used, the Active Directory page in the ACS GUI slows down. **Conditions** The ACS server has at least two DNS servers configured. This issue occurs when the primary DNS server is not functioning or is not accessible. **Workaround** To avoid this issue, configure the secondary DNS server as the primary DNS server.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw49239	ACS is deleted from Active Directory during restart.	**Symptom** When ACS is restarted, it is deleted from the Active Directory server and then reconnected. **Conditions** The ACS machine is deleted from the Active Directory server and then reconnected when: • ACS is restarted. • The Active Directory configuration is modified. **Workaround** To avoid this issue, you must add the ACS machine to the Active Directory server earlier. **Note** ACS patch 5.0.0.21.3 contains a fix for this issue.
CSCsw51074	Unable to restore the purge backup in the VMWare setup.	**Symptom** When database purging is initiated, a data backup is performed. When the **acs restore** command is used to restore the data, the backup file is not restored. **Conditions** This issue occurs when you try to restore the backup file created during database purging. **Workaround** To avoid this issue, you must perform a manual backup using the **acs backup** command via the CLI.
CSCsw51098	Replication from deregistered Secondary server must be blocked.	**Symptom** When an offline Secondary server is deregistered, the Secondary server receives Full Replication updates once it appears online. **Conditions** When the Secondary server is offline, it does not deregister from the Primary and remains in the Secondary mode. When the Secondary server appears online, you can perform a Full Replication on the Secondary server, but a Full Replication must not be performed in this state. **Workaround** When the Secondary server appears online, navigate to the Secondary GUI and deregister it from the Primary.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw51685	Unable to access the ACS GUI after installing patch 5-0-0-21-1	**Symptom** The GUI login page gets hung and displays the following error message: `You have just initiated a software update, please wait until the software update has completed. ACS is unavailable, please wait.` **Conditions** This issue occurs when you perform a software upgrade or install a patch via the GUI using incorrect upgrade data or a file that does not exist. **Workaround** To avoid this issue, you must close the browser and reopen it. Verify that the upgrade or patch is installed from the CLI. If it is not installed from the CLI or GUI, you must perform the installation process again.
CSCsw63978	The software repository and software update objects must be validated.	**Symptom** When downloading a patch from a repository via the GUI, if the URL field contains an extra space, the patch download fails. **Conditions** This issue occurs when installing a patch for the ACS 5.0 version. **Workaround** To cancel the upgrade: 1. Open a new window and log in to the ACS GUI. 2. Navigate to the **Distributed Management** tab and click the **Edit** button to cancel the software update process. 3. Enter a valid URL that does not contain spaces and install the patch.
CSCsw75401	Cores in TACACS during stress when configuring LDAP with non existent IP.	**Symptom** During TACACS+ stress and abnormal traffic, ACS restarts. **Conditions** This issue occurs during TACACS+ stress and abnormal traffic, but it does not always occur. **Workaround** ACS automatically restarts.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw78205	Custom date on RADIUS and TACACS session directory must be restricted.	**Symptom** When you select a custom time range for the following reports: • RADIUS_Session_History • TACACS_Session_History • RADIUS_Session_Lookup • TACACS_Session_Lookup You can select a time range that is greater than 30 days, even when the session history is archived for only the previous 30 days. **Conditions** This issue occurs when you select a custom time range for these reports. **Workaround** To avoid this issue, you must select a time range that is equal to, or less than, 30 days.
CSCsw79771	System error in Device Admin Policy	**Symptom** The GUI displays the following error message above the policy table: `This System Failure occurred: {0}. Your changes have not been saved. Click OK to return to the list page.` **Conditions** 1. Navigate to **Access Policies > Access Services > Default Device Admin > Authorization**. 2. Ensure that only the shell profile result is visible. 3. Launch the default dialog window and choose a shell profile as the result for the default role. 4. Click **OK**. 5. Click **Customize** and add the command set to the list of selected results. 6. Click **OK**. 7. Click **Save Changes** to submit the changes. This issue occurs for other Access Services when: • The default rule and a set of selected results are modified. • Both changes are saved simultaneously. **Workaround** To avoid this error, you must: • Perform the operations separately. • First submit a default value change and then customize the results.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw79961	Some records are not present when inserting multiple user records.	**Symptom** When multiple users simultaneously perform many configuration, a small number of objects that are to be added to the ACS configuration are not added. **Conditions** This issue occurs when all of the following are done: 1. The automated stress tool is used. 2. Ten administrators simultaneously perform many configuration activities. 3. Some of the administrators add network devices, MABs, and internal users. 4. Other users view pages or log in and log out of ACS. **Workaround** To avoid this issue, you must: • Avoid using automated tools via the GUI. • Perform all configurations manually.
CSCsw79994	If Auto Activation is disabled, Secondary displays incorrect deployment status.	**Symptom** When Auto Activation is disabled: • A registered Secondary server becomes inactive. • Contains an odd state when it is viewed from the Secondary GUI. **Conditions** When Auto Activation is disabled, a registered Secondary server becomes inactive and stops receiving Full Replication updates from the Primary. The Secondary server GUI displays the deployment state of the Secondary server as it was before the registration. Once the Secondary server is active, this state is replaced with the configuration from the Primary. **Workaround** From the Primary GUI, you must activate the Secondary server to update it with the deployment configuration.
CSCsw80025	Primary is not updated after inactive Secondary server is deregistered.	**Symptom** When a Secondary server is set to inactive in the Primary, it can be deregistered from the Secondary server, but this state is not updated to the Primary. **Conditions** When a Secondary server is set to inactive in the Primary: • This state is not updated to the inactive Secondary server. • Promotion and FullSync are not blocked. • De-registration is not sent back to the Primary. **Workaround** If de-registration is performed from the Secondary server, you must manually deregister the node from the Primary.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw80029	If Auto Active is disabled, the Secondary server GUI should not display the restart message.	**Symptom** When the Secondary server is inactive, the GUI restart message should not be displayed. **Conditions** After registration with the Primary, the Secondary server GUI displays a Secondary server restart message. This message should not be displayed, as a restart is not required and the node is inactive in the Primary. **Workaround** Please ignore this message and log in to the GUI.
CSCsw80364	When the Primary is set to Local Mode, inactive Secondary server cannot update it.	**Symptom** When the Primary is set to Local Mode, the inactive Secondary server cannot update it. **Conditions** If a Secondary server is inactive, deregistration and Local Mode switching in the Secondary server is not reported to the Primary, as the Secondary server cannot communicate with the Primary. **Workaround** A workaround is not required, as the Secondary server operates properly in Local Mode. If the Secondary server has to rejoin the deployment, the Secondary node must be deregistered in the Primary GUI.
CSCsw80396	Installation of CA fails if CRL cannot be parsed.	**Symptom** Addition of a CA fails. **Conditions** When a CA is added, the CRL field is parsed to define the initial CRL for the certificate. If a certificate contains CRL information that does not begin with http://, the addition of this CA fails and the following error is displayed: `Certificate is not valid.` This issue occurs as ACS supports a CRL that begins with only with http://. **Workaround** None. **Note** ACS 5.0 patch 3:5.0.0.21.3 contains a fix for this issue.
CSCsw80431	Secondary server is not updated after being deactivated from the Primary.	**Symptom** After a Secondary server is deactivated from the Primary, the Secondary server is not updated. **Conditions** The state of the Secondary server is not updated to the Primary, as an inactive Secondary server cannot communicate with the Primary. **Workaround** A workaround is not required.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw80531	The option of activating an inactive Secondary server that is offline, must be disabled.	**Symptom** The option of activating an inactive Secondary server that is offline, must be disabled. **Conditions** If an inactive Secondary server is offline and is activated in the Primary, this updated state is not communicated to the Secondary server and it continues to remain inactive. **Workaround** You must activate the Secondary server from the Primary GUI after the Secondary server appears online. **Note** When a Secondary server is inactive, its online state is not communicated to the Primary GUI.
CSCsw80602	After changing hostname ACS continues authorization with old hostname.	**Symptom** When the ACS hostname is changed, ACS is still connected to the Active Directory domain with the old hostname. **Conditions** This issue occurs when the ACS hostname is changed while ACS is connected to the Active Directory domain. **Workaround** To avoid this issue, you must: 1. Navigate to the Active Directory configuration page. 2. Delete the Active Directory configuration. 3. Redefine the Active Directory configuration.
CSCsw80835	Primary is not updated if registered from Secondary server Local Mode.	**Symptom** If a node is registered to another Primary while it is in Local Mode, the old Primary continues to display the node in Local Mode. **Conditions** This issue occurs as systems in Local Mode function separately and stop updating their Primary with changes in Role. **Workaround** To avoid this issue, you must delete the Local Mode system from the Old Primary Instance Listing page.
CSCsw81667	Open ACS TCP ports are vulnerable to TCP established attacks.	**Symptom** When an established TCP attack is performed against open TCP ports in ACS, ACS fails. This DoS attack is performed by an internal attacker, assuming that ACS is in the Demilitarized Zone (DMZ). **Conditions** This issue occurs when multiple TCP connections are opened and not closed. **Workaround** This issue can be avoided by using a firewall, which prevents attackers from directly connecting to the ACS network.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw87851	If the Log Collector is set on a deregistered ACS, View stops.	**Symptom** If the Log Collector is enabled on a deregistered ACS, the Log Collector stops on the Primary. **Conditions** If the Log Collector is enabled on the Primary and a deregistered Secondary server is chosen as the Log Collector, the following error is displayed: `Deregistered Secondary cannot be selected` and the Log Collector on the Primary stops. **Workaround** To avoid this error, you must restart ACS on the Primary.
CSCsw88053	If the Log Collector is set for an offline Secondary server, Monitoring and Reporting is disabled.	**Symptom** If the Log Collector is set on an offline Secondary server, the Log Collector stops running in the deployment. **Conditions** If a Secondary server is offline, it stops receiving Log Collector replication updates when it appears online. This stops the Log Collector in the deployment. **Workaround** To avoid this issue, you must perform a Full Replication for the Secondary server when it appears online.
CSCsw90173	If the Log Collector is set for an inactive Secondary server, Monitoring and Reporting is disabled.	**Symptom** If the Log Collector is set on an inactive Secondary server, Monitoring and Reporting is disabled. **Conditions** When a Secondary node is inactive, it stops receiving replication updates from the Primary. If the Log Collector is set on an inactive Secondary server, it stops receiving configuration updates from the Primary and fails to start the Log Collector. **Workaround** To avoid this issue, you must activate the Secondary server from the Primary GUI.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsw90830	If the patch install fails, an incorrect error is displayed.	**Symptom** When you install a patch via the CLI using the **acs patch install** command, if the installation process fails, the prompt displays the following error message: `shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory` and the ACS server fails to restart. **Conditions** The installation process fails if the patch is installed on one of the following: • An ACS version that is not supported. • A corrupted ACS, which is a rare case. **Workaround** If the installation fails, you must check the status of ACS using the **show application status acs** command. If ACS is not running, you must enter the **acs start command** to restart ACS.
CSCsw92788	When the node is deregistered, every node logging configuration is reset.	**Symptom** When a node deregisters and reregisters, the configuration for each instance log category is deleted. **Conditions** There is a global set of log category definitions which you can override for a specific Secondary ACS instance, and then recreate definitions specific to that instance. If instance-specific definitions are deregistered and re-registered, the definitions are deleted. **Workaround** There is no regular workaround for this. However, you can record the specific log configuration definitions for the ACS instance that is deregistered, and manually restore them when the instance is re-registered.
CSCsw93693	ACS fails to respond to multiple **cts-rbacl attr** in a single RADIUS request.	**Symptom** ACS downloads only a single SGACL value. **Conditions** This issue occurs when you request multiple SGACLs in a single RADIUS request. **Workaround** For every RADIUS request, the device should send only a single SGACL download request.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCsx02429	Invalid UPN domain name is deleted during EAP authentication against Active Directory.	**Symptom** When authenticating against Active Directory, if you use a UPN a valid username, but an invalid domain name, the invalid domain name is deleted and the authentication is performed using only the username. This issue occurs when performing authentication with only EAP and not with RADIUS PAP. **Conditions** Performing an EAP authentication against Active Directory with an invalid domain in UPN format. **Workaround** None.
CSCta44581	Intel supplicant cannot authenticate with expired PAC.	**Symptom** When an Intel supplicant tries to authenticate with an expired PAC, the authentication does not succeed and the PAC is never replaced. Intel supplicant sends EAP-FAST hello message with an expired PAC. ACS answers with a server hello message and sends a certificate with this message. ACS tries to start anonymous reauthentication since the PAC has expired. Intel receives the ACS server hello message and sends back a TLS fatal alert “unexpected message” and the session ends. **Conditions** This issue occurs every time an Intel supplicant tries to authenticate with an expired PAC. **Workaround** To notify the supplicant that there is a problem with the session, ACS must send a TLS alert to the supplicant for the supplicant to end the session and start a new one.
CSCta56356	Odyssey authentication with blank username results in invalid payload.	**Symptom** When authenticating with Odyssey, if the username field is empty, the request is dropped with the following message in the Monitoring and Report Viewer: `Invalid inner-EAP payload dropped.` **Conditions** This issue occurs when you use an Odyssey client for password-based authentication and the username field is empty. **Workaround** You must go to the Odyssey WiFi screen and disable the Connect to the Network option to change the username in the Profile.

Table 2 Known Caveats in ACS 5.0 (continued)

Bug ID	Summary	Explanation
CSCta53582	Case where customer log:11523 should be "rejected" not "dropped".	**Symptom** After authentication with Odyssey, the log in the Monitoring and Report Viewer server contains the following log message instead of describing the authentication as rejected: `11523 invalid inner EAP payload dropped` **Conditions** This issue occurs when you use an Odyssey client for password-based authentication and the username field is empty. **Workaround** You must go to Odyssey WiFi screen and disable the Connect to the Network option to change the username in the Profile. You cannot change the text of the message.

CSCta58340	PEAP authentication with wrong password results in Invalid EAP Payload on CSSC XP supplicant.	**Symptom** When using CSSC 5.1 on an XP supplicant, if you authenticate with an incorrect password, the following message appears on CSSC 5.1:
		`Password was incorrect for the network. Please try again.`
		When you get the above error message, wait for 30 seconds before you re-enter your credentials. Several lines of the following message are logged in the Monitoring and Report Viewer server:
		`11500 Invalid EAP Payload Dropped`
		Conditions This issue occurs during PEAP authentication against a user who uses an incorrect password.
		Workaround Provide the correct credentials when requested by the supplicant.

CSCtb57469	Dialin permission check box not available.	**Symptom** ACS 5 does not have a built-in check box for the dial-in permission attribute for Windows users. **Conditions** The Windows Dialin Permission feature is not supported. **Workaround** Check the attribute msNPAllowDialin via LDAP or Windows Active Directory.

Documentation Updates

Table 3 Updates to Release Notes for ACS 5.0

Date	Description
7/10/09	**Omissions:** In the online *User Guide for the Cisco Secure Access Control System 5.0 and Installation Guide for the Cisco 1120 Secure Access Control System 5.0,* the following information was omitted: Before importing a module, you must ensure that the import progress pop-up window will be displayed. To ensure this, you must do one of the following: • Disable the pop-up blocker for ACS. • Add an exception to allow pop-ups only for ACS. • Verify that the browser settings are restored to their default settings. If the pop-up blocker is enabled for ACS, the following problems are encountered: • If the import file is valid, the import process begins but the progress pop-up window will not be displayed. You will have to refresh the target list to view the newly imported items. • If the import file is not valid, the log message for this is not displayed.
10/8/09	**Unsupported features for ACS 5.0:** • Network access restriction to users whose Windows accounts have Windows dial-in permission. • IP Pools Server feature. • Support for defining the maximum number of simultaneous sessions for a user or user group.
10/8/09	**Included a known caveat for ACS 5.0:** • CSCtb57469—Dialin permission check box not available.

Product Documentation

Table 4 describes the product documentation that is available for ACS 5.0.

Table 4 Product Documentation

Document Title	Available Formats
Documentation Guide for the Cisco Secure Access Control System 5.0	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/roadmap/ACS50roadmap.html
Regulatory Compliance and Safety Information for the Cisco 1120 Secure Access Control System 5.0	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/regulatory/compliance/csacsrcsi.html
User Guide for the Cisco Secure Access Control System 5.0	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/user/guide/ACS_user_guide.html

Table 4 Product Documentation (continued)

Document Title	Available Formats
Installation Guide for the Cisco 1120 Secure Access Control System 5.0	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/installation/guide/ACS5.0_Install.html
Migration Guide for the Cisco Secure Access Control System 5.0	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/migration/guide/migrationguide.html
CLI Reference Guide for the Cisco Secure Access Control System 5.0	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/command/reference/ACS_CLI_guide.html
Supported and Interoperable Devices and Software Tables for the Cisco Secure Access Control System 5.0	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/device_support/sdt50.html
Release Notes for the Cisco Secure Access Control System 5.0	http://www.cisco.com/en/US/products/ps9911/prod_release_notes_list.html

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Supplemental License Agreement

END USER LICENSE AGREEMENT SUPPLEMENT FOR CISCO SYSTEMS ACCESS CONTROL SYSTEM SOFTWARE:

IMPORTANT: READ CAREFULLY

This End User License Agreement Supplement ("Supplement") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this Supplement but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this Supplement, the terms and conditions of this Supplement will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this Supplement. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

1. Product Names

For purposes of this Supplement, the Product name(s) and the Product description(s) you may order as part of Access Control System Software are:

A. Advanced Reporting and Troubleshooting License

Enables custom reporting, alerting and other monitoring and troubleshooting features.

B. Large Deployment License

Allows deployment to support more than 500 network devices (AAA clients that are counted by configured IP addresses). That is, the Large Deployment license enables the ACS deployment to support an unlimited number of network devices in the enterprise.

C. Advanced Access License (not available for Access Control System Software 5.0, will be released with a future Access Control System Software release)

Enables TrustSec policy control functionality and other advanced access features.

2. ADDITIONAL LICENSE RESTRICTIONS

- Installation and Use. The Cisco Secure Access Control System(ACS) Software component of the Cisco 1120 Hardware Platform is pre installed. CD's containing tools to restore this Software to the 1120 hardware are provided to Customer for reinstallation purposes only. Customer may only run the supported Cisco Secure Access Control System Software Products on the Cisco 1120 Hardware Platform designed for its use. No unsupported Software product or component may be installed on the Cisco 1120 Hardware Platform.
- Software Upgrades, Major and Minor Releases. Cisco may provide Cisco Secure Access Control System Software upgrades for the 1120 Hardware Platform as Major Upgrades or Minor Upgrades. If the Software Major Upgrades or Minor Upgrades can be purchased through Cisco or a recognized partner or reseller, the Customer should purchase one Major Upgrade or Minor Upgrade for each Cisco 1120 Hardware Platform. If the Customer is eligible to receive the Software release through a Cisco extended service program, the Customer should request to receive only one Software upgrade or new version release per valid service contract.
- Reproduction and Distribution. Customer may not reproduce nor distribute software.

3. DEFINITIONS

Major Upgrade means a release of Software that provides additional software functions. Cisco designates Major Upgrades as a change in the ones digit of the Software version number [(x).x.x].

Minor Upgrade means an incremental release of Software that provides maintenance fixes and additional software functions. Cisco designates Minor Upgrades as a change in the tenths digit of the Software version number [x.(x).x].

4. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

Please refer to the Cisco Systems, Inc., End User License Agreement.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Release Notes for the Cisco Secure Access Control System 5.0